RSAC 2025 Conference

Many Voices. One Community.

SESSION ID: PART2-T09

Proactive Insider Threat Management: A Real-World Case Study

David Pinckard

VP of Product
Teramind

Justin Skagen CFE

Executive Director of Revenue Integrity and Fraud
Arrivia

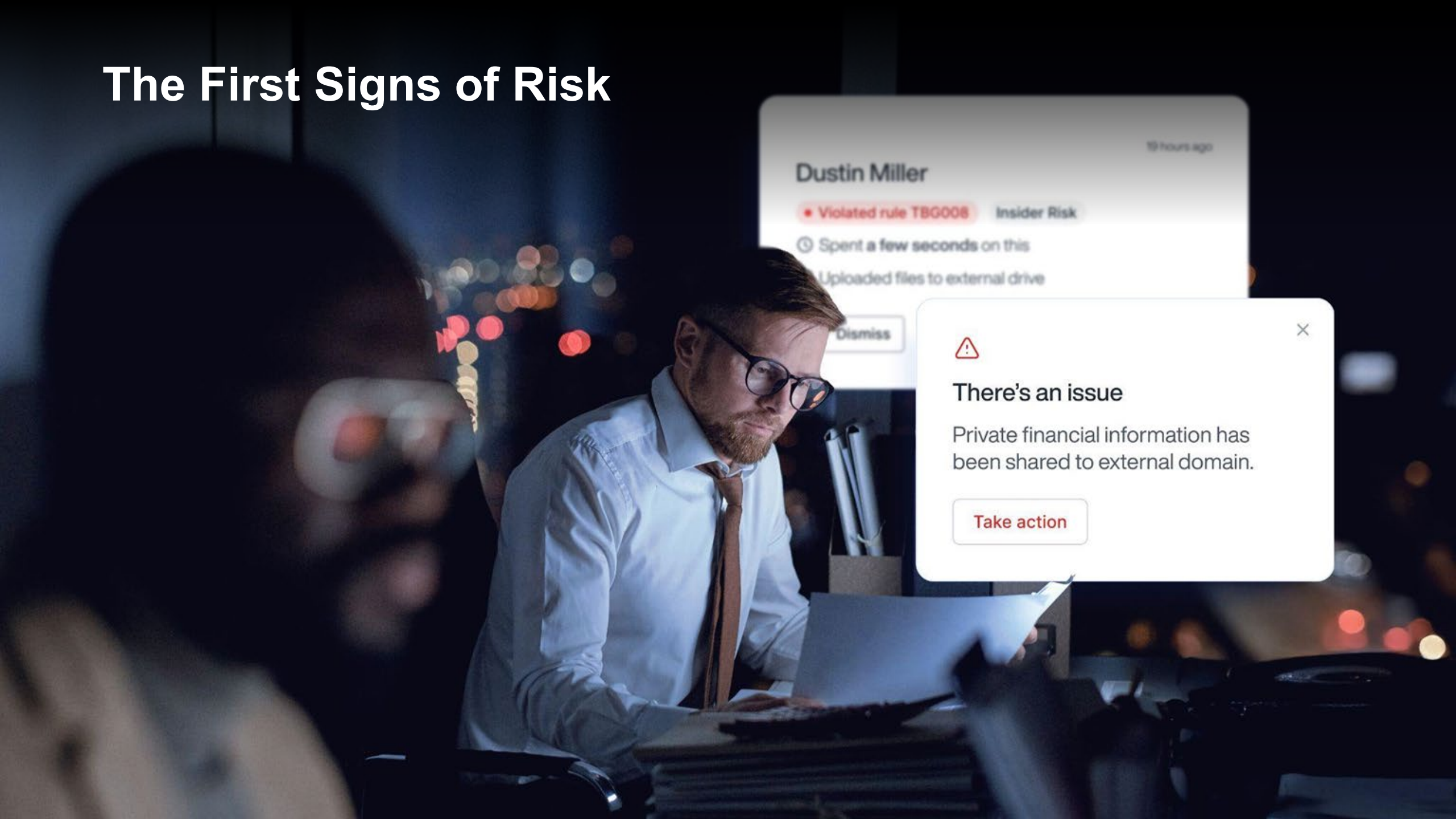
Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

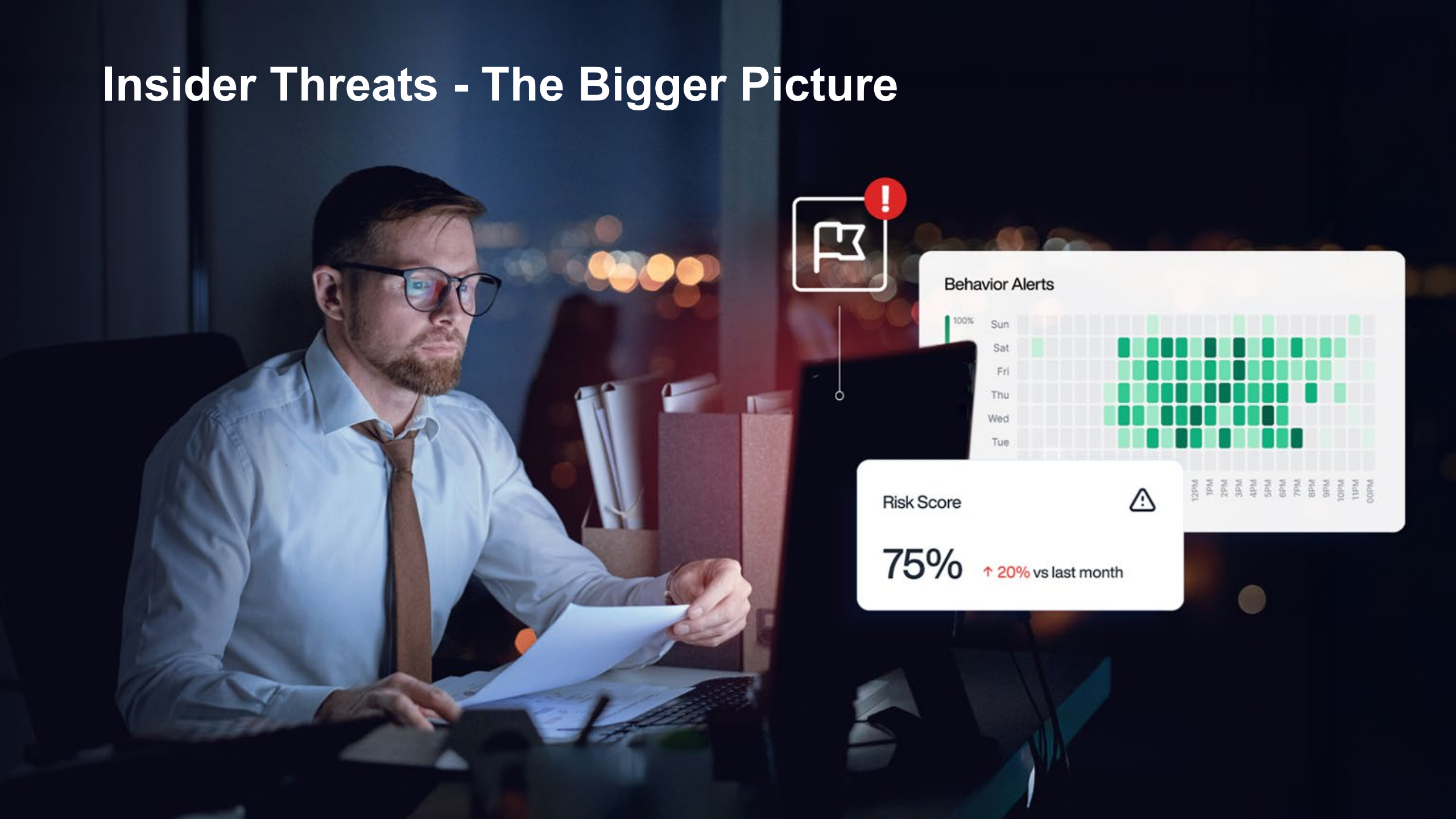
Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

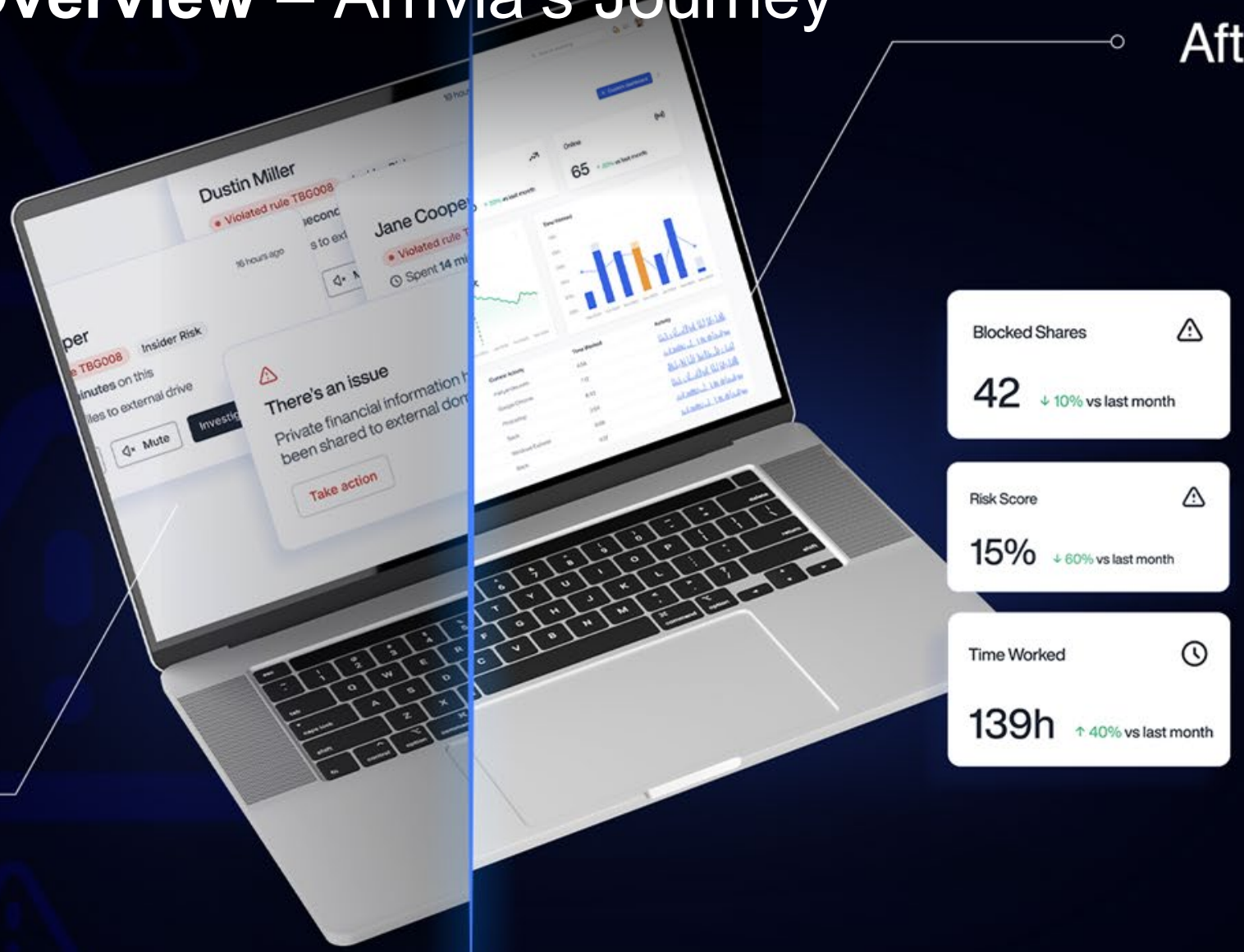
The First Signs of Risk



Insider Threats - The Bigger Picture



Case Study Overview – Arrivia's Journey

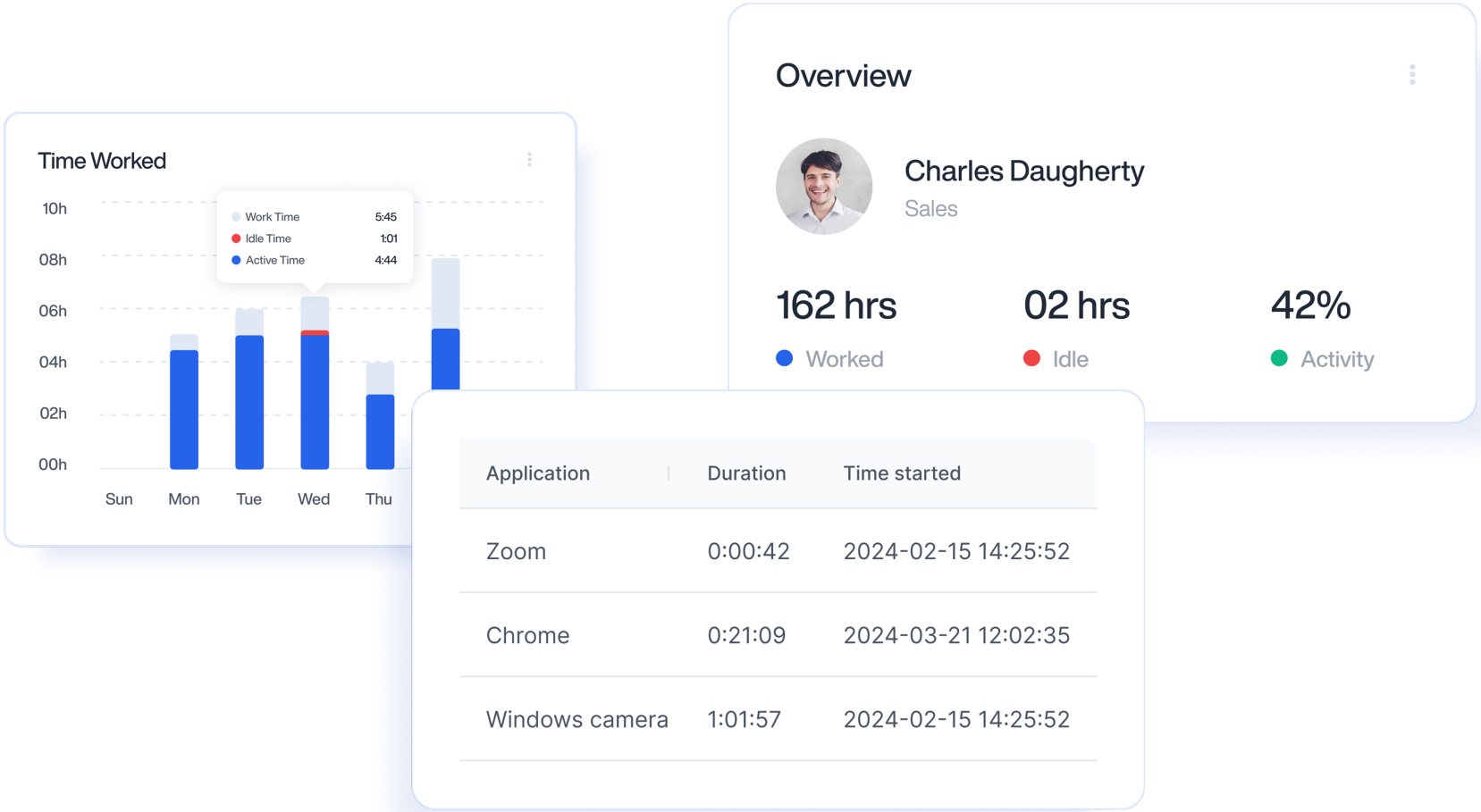


After

Before

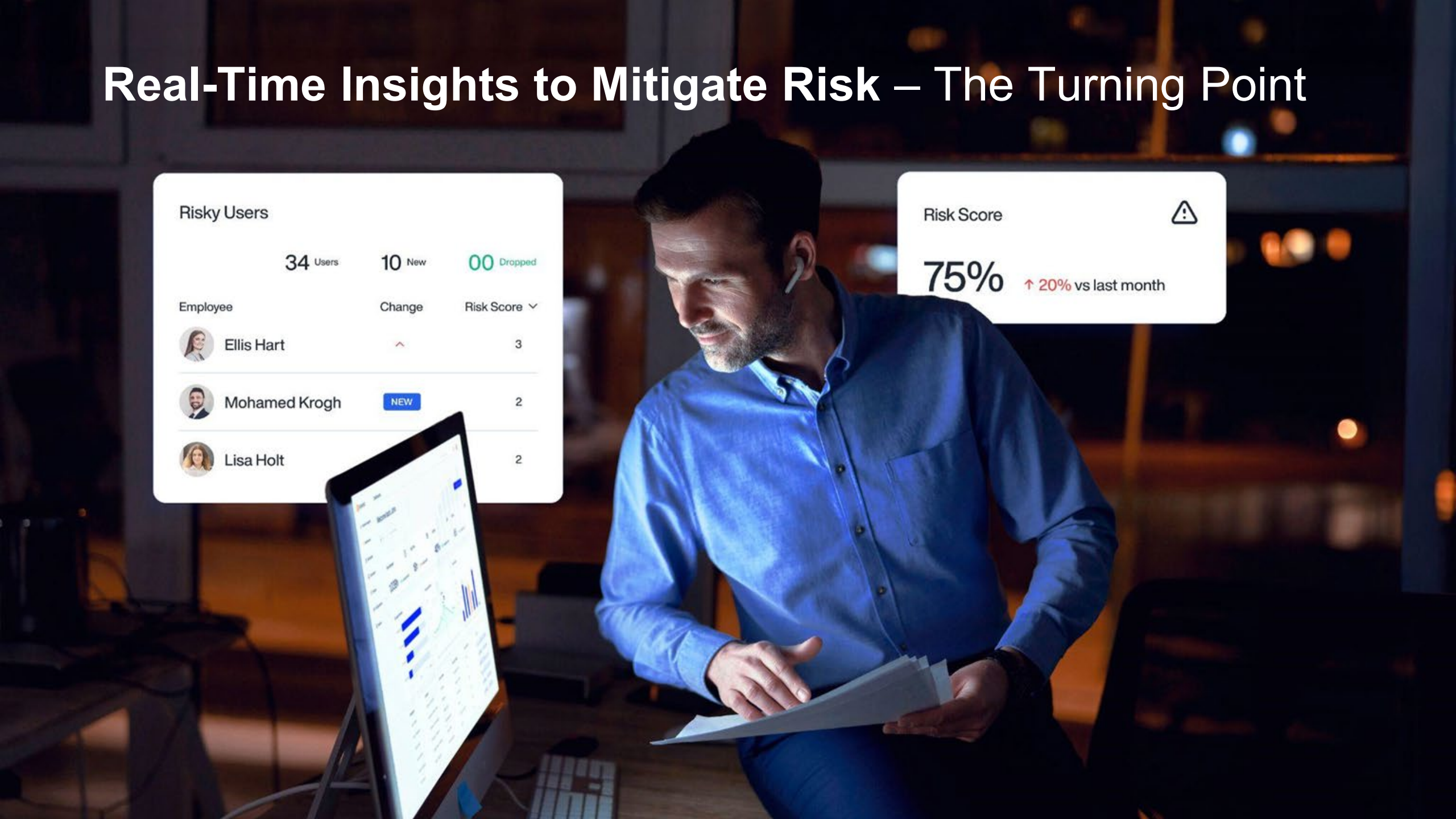
TERAMIND | arrivia

Phase 1 – Small-Scale Pilot (20 Employees)



Phase 2 – Scaling to 1,500+ Employees

Real-Time Insights to Mitigate Risk – The Turning Point



Balancing Security & Employee Trust – The Challenge

Arrivia Security Use Cases – Fraud Investigations

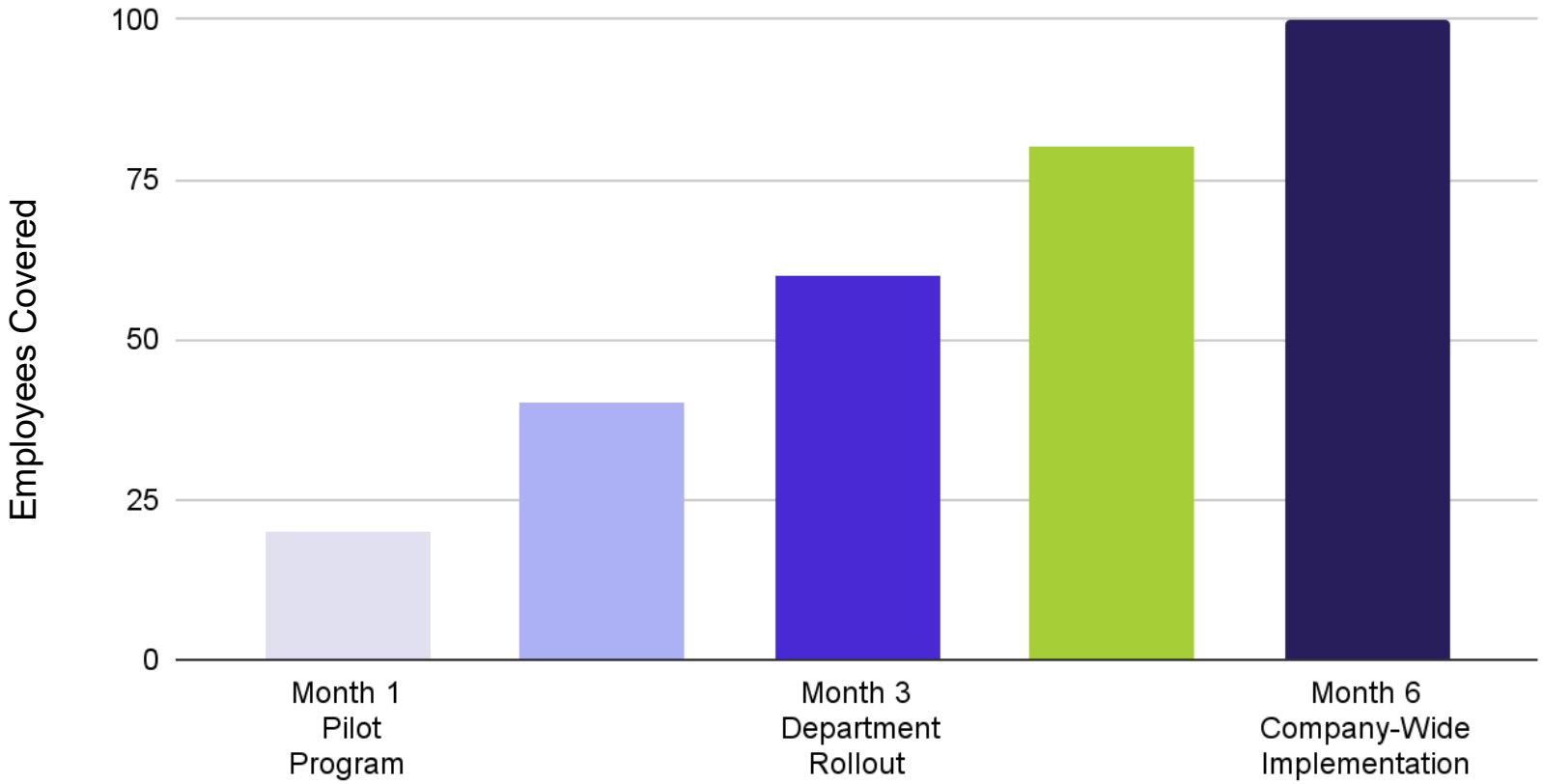
Recognizing & Rewarding Top Performers

Insider Threats: Beyond Data Theft

- **Fraudulent Sick Leave**
- **Fake System Issues**
- **Manipulated Time Tracking**

Streamlining Fraud Investigations – The Payoff

Scaling Insider Threat Management – The Impact



Key Lessons – The Big Takeaways

Threat Detection

Behavioral analytics are essential.

Employee Trust

Employee trust must be maintained.

Risk Mitigation

Real-time threat detection prevents damage.

Apply It – What You Should Do Next

- **Next Week:**
  - Conduct a quick risk assessment (e.g., identify critical data assets).
  - Set up a small-scale pilot or proof-of-concept with a targeted team.
- **Next 3 Months:**
  - Expand monitoring and DLP tools across multiple departments.
  - Begin formalizing policies and procedures for insider threat response.
  - Establish cross-functional buy-in (HR, Legal, Compliance).
- **Next 6 Months:**
  - Fully integrate behavioral analytics into your security ecosystem.
  - Regularly review and update your insider threat program based on data insights.
  - Foster a culture of transparency and continuous improvement.

RSAC 2025 Conference

Many Voices.
One Community.

Q & A

Visit Teramind at Booth N - 6044.